UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/611,402	06/30/2003	Winefred Washington	013628.00499 (02CXT0078D)	1911

77339 7590 04/04/2008		

JACKSON WALKER (CONEXANT)
901 MAIN STREET, SUITE 6000
DALLAS, TX 75202

EXAMINER
JACKSON, JENISE E

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
04/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/611,402	WASHINGTON, WINEFRED
Office Action Summary	Examiner	Art Unit
	JENISE E. JACKSON	2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>24 March 2008</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-5,7-15 and 17-27</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-5,7-15 and 17-27</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date <u>20040427</u>.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/27/07

has been entered.

2.   Claims 1, 3-4, 7-9, 10, 13, 18, 22, 25, 27 have been amended by Applicant to

correct lack of antecedent basis in certain claims. Claims 1-5, 7-15, 17-27 are pending.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4.   Claims 1-5, 7-15, 17-27 are rejected under 35 U.S.C. 102(e) as being anticipated

by Driscoll(6,763,363).

5.   As per claim 1, Driscoll discloses an encryption key generator(col. 5, lines 15-17,

fig. 1 sheet 1); a data buffer(col. 7, lines 61-67, col. 8, lines 1-5); an input/output register

that interfaces with memory of the digital device(see fig. 1 sheet 1, fig. 2 sheet 2, see col.

6, lines 38-46), and a memory controller that directs digital data from the memory to the

data buffer with the digital data passing thorough the encryption key generator prior to

entering the input/output register(see fig. 1 sheet 1, fig 2 sheet 2, col. 4, lines 30-46).

6.   As per claim 2, Driscoll discloses a clock(see col. 6, lines 31-34); a key store(fig.

1 sheet 1); and a linear feedback shift register(see fig. 2 sheet 2) generates a

pseudorandom bit pattern while the linear feedback shift register is enabled and stores a

plurality of bits as at least one key in the key store(see col. 3, lines 46-52, col. 4, lines 31-

46).

7.   As per claim 3, Driscoll discloses where the encryption key generator further

includes a random number generator that receives the pseudorandom bit pattern from the

linear feedback shift register and provides a random number for use by the digital

device(fig. 1 sheet 1, fig. 2 sheet 2, col. 4, lines 47-51).

8.   As per claim 4, Driscoll discloses pseudorandom bit pattern that creates a bit

stream; and a key store that stores portions of pseudorandom bit pattern as the at least one

keys(see col. 3, lines 46-51, col. 4, lines 30-36, fig. 1 sheet 1).

9.   As per claim 5, Driscoll discloses including a pseudo random number generator

that selects a portion of the pseudorandom bit pattern to be random number(see col. 3,

lines 46-64).

10.   As per claim 7, Driscoll discloses a subkey that creates a sub-key based on data

from the memory controller and a selected key from the key store; and a combiner that

combines the sub-key with the digital data(col. 7, lines 25-32).

11.   As per claim 8, Driscoll discloses a data mixer that mixes the bits of a byte of

digital data; and a combiner that combines the byte of the digital data prior to the byte

being combined with the sub-key(fig. 1 sheet 1, col. 4, lines 3-46, col. 7, lines 25-32).

12.   As per claim 9, Driscoll discloses a memory controller that generates a memory

request to retrieve the encrypted digital data; and encryption circuit with a plurality of

key that decrypts the encrypted digital data in response to the memory request of the

memory controller(see fig. 1 sheet 1, col. 5, lines 33-55).

13.   As per claim 10, Driscoll discloses a combiner that combines one of the plurality

of keys with a bank and row information contained in the memory request resulting in a

sub-key(fig. 1 sheet 1, col. 4, lines 3-46, col. 7, lines 25-32).

14.   As per claim 11, Driscoll discloses a data mixer that unmixes bits within a byte

after the sub-key is applied to encrypted digital data(see fig. 1 sheet 1, col. 4, lines 3-46,

col. 4, lines 3-46, col. 5, lines 33-55).

15.   As per claim 12, Driscoll discloses generating at least one key, placing the digital

data in a data buffer; and encrypting the digital data using the at least one key while the

digital data is being placed(see col. 3, lines 46-64, col. 5, lines 25-32, col. 8, lines 22-32).

16.   As per claim 13, Driscoll discloses generating of a clock signal(see col. 6, lines

31-34), creating a pseudorandom bit pattern, and storing at least one portion of the

pseudorandom bit pattern in a key store as the at least one key(see col. 3, lines 46-51, col.

4, lines 30-36, fig. 1 sheet 1).

17.   As per claim 14, Driscoll discloses where the pseudorandom bit pattern is

generated by a linear feedback shift register(fig. 1 sheet 1, fig. 2 sheet 2, col. 4, lines 47-

51).

18.   As per claims 15, 21, Driscoll discloses generating a random number from the

pseudorandom bit pattern(fig. 1 sheet 1, fig. 2 sheet 2, col. 3, lines 46-64).

19.   As per claim 17, Driscoll discloses selecting a portion of the pseudorandom bit

pattern to be used a random number(col. 3, lines 46-54, col. 5, lines 14-24).

20.   As per claim 18, Driscoll discloses mixing the bits of a byte of the digital data

with a data and combining the byte with the at least one key(fig. 1 sheet 1, col. 4, lines

30-46).

21.   As per claim 19, Driscoll discloses generating a sub-key with data from the

memory controller and the key; and combining the sub-key with the digital data(col. 7,

lines 25-32).

22.   As per claim 20, Driscoll discloses mixing the bits of byte of digital data with a

data mixer; and combining the byte with the sub-key(fig. 1 sheet 1, col. 4, lines 3-46, col.

7, lines 25-32).

23.   As per claim 22, Driscoll discloses generating a memory request to retrieve the

encrypted digital data; and decrypting the encrypted digital data using at least one

key(see fig. 1 sheet 1, col. 5, lines 15-55).

24.   As per claim 23, Driscoll discloses combining the at least one key with a bank and

row information contained in the memory request to generate a sub-key(col. 8, lines 21-

63).

25.   As per claim 24, Driscoll discloses unmixing a byte of encrypted digital data with

a data mixer(see col. 5, lines 33-55).

26.   As per claim 25, Driscoll discloses an encryption circuit with at least one key(fig.

1 sheet 1, col. 5, lines 15-24); a data buffer filled with the digital data(see col. 7, lines 60-

67, col. 8, lines 1-5), a memory controller that directs and the storage of digital data in the

rewriteable memory with the digital data being encrypted by the encryption circuit and

the at least one key after the digital data has entered the data buffer but prior to being

stored in the rewritable memory(see fig. 1 sheet 1, fig 2 sheet 2, col. 4, lines 30-46).

27.   As per claim 26, Driscoll discloses a pseudorandom bit stream generator that

creates a pseudorandom bit stream; and a key store that stores the at least one key that is

selected from the pseudorandom bit stream(col. 3, lines 46-54).

28.   As per claims 27, Driscoll discloses a data mixer mixes the bits of a byte of the

digital data(fig. 1 sheet 1); and a combiner(26) that combines the byte with the key(fig. 1

sheet 1, col. 4, lines 30-46).

Response to Applicant

28.   The Applicant states that Driscoll does not disclose encryption of digital data in

memory of a digital device. The Examiner disagrees with the Applicant. Driscoll

performs encryption of digital data in a computer, because Driscoll discloses the

sender(see col. 5, lines 15-24) includes a pseudo-random number generator (PRNG) and

an encryption combiner, the PRNG receives a private key which controls PRNG to

produce an encryption keystream(see col. 5, lines 14-25). Plaintext(i.e. digital data) is

provided to encryption combiner, and encryption combiner combines the plaintext and

encryption keystream to form ciphertext(see col. 5, lines 25-30).

29.   The Applicant states that Driscoll does not disclose a data buffer into which the

memory controller directs data to be encrypted or decrypted. The Examiner disagrees

with the Applicant. Driscoll discloses the temporary storage word(i.e. buffer) is left

shifted by one-bit location to shift a zero into the LSB of temporary storage word(see col.

7, lines 60-66). The temporary word resulting from the XOR linear feedback function is first stored in the temporary storage word(see col. 8, lines 23-32, fig. 2 sheet 2).

30.   The Applicant states that Driscoll does not disclose an input/output register. The Examiner disagrees with the Applicant. Driscoll discloses the pseudo random number generator(PRNG) includes a linear feedback shift register(LFSR). The LFSR includes n storage elements and a linear function that loads data to generate a keystream sequence(see col. 6, lines 6-13). The output register in Driscoll is that the LFSR output is provided from the most significant word(see col. 6, lines 38-46).

31.   The Applicant states that Driscoll does not disclose a memory controller that directs digital data to the data buffer with digital data passing through the encryption key generator prior to entering the input/output register. The Examiner disagrees with the Applicant. Driscoll discloses a PRNG includes a word-by-word shifting LFSR for providing a LFSR output word of word length M. The stream cipher cryptosystem also includes a cryptographic combiner for combining a first binary data sequence and the keystream to provide a second binary data sequence(see col. 4, lines 30-40).

32.   The Applicant states that Driscoll does not disclose a memory controller capable of generating a memory control signal that is used to write digital data to rewriteable memory after that digital data is encrypted in an encryption circuit. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JENISE E. JACKSON whose telephone number is (571)272-3791. The examiner can normally be reached on Increased Flex time, but generally in the office M-Fri(8-4:30)..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. E. J./
Examiner, Art Unit 2139

March 26, 2008

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139